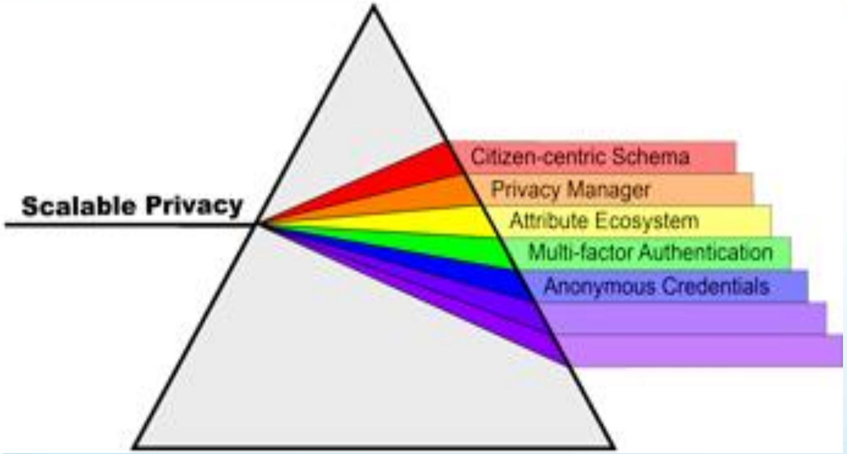
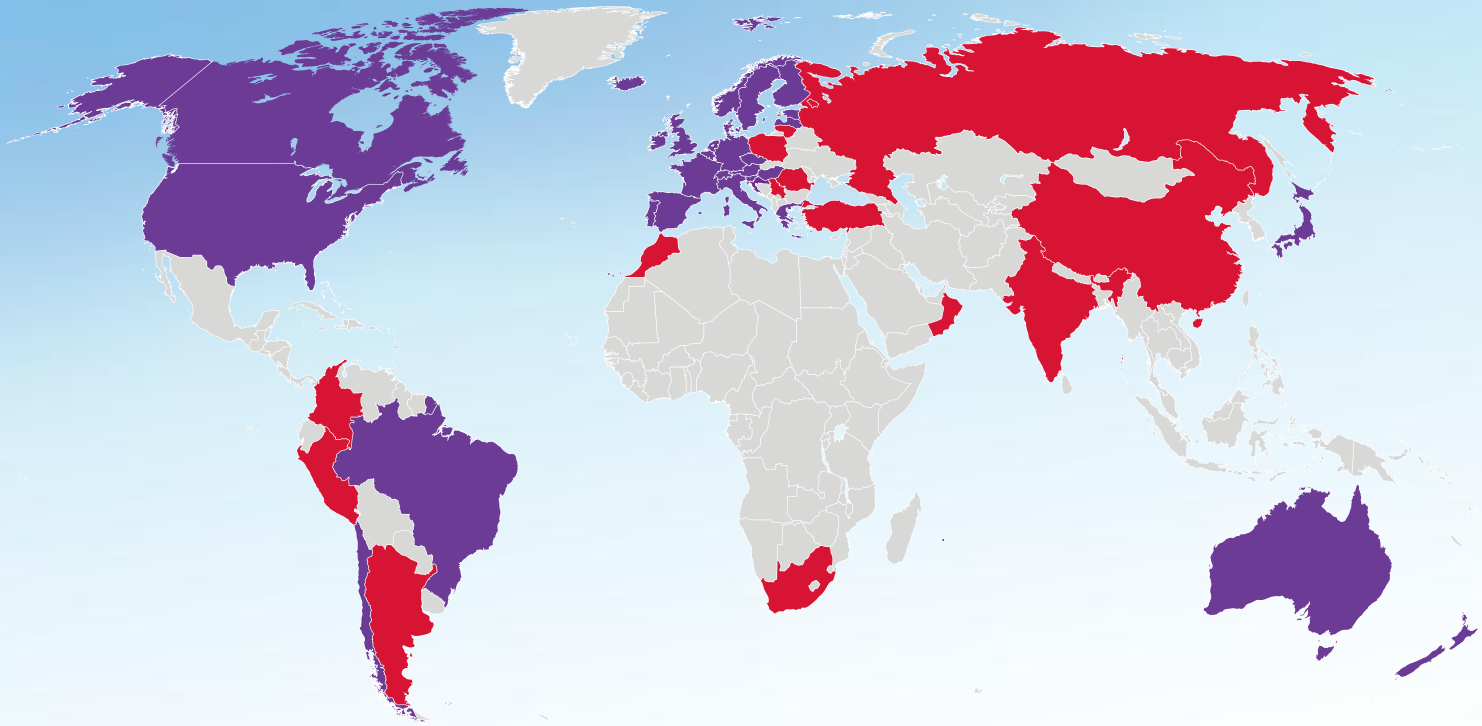


Scalable Privacy

Topics

- Context
  - R&E federations globally
  - InCommon
- Scalable Privacy
  - MFA Deliverables
  - Citizen-centric attribute deliverables
  - Privacy managers
  - Anonymous credentials
  - In support of trust
    - Periodic table of trust elements
    - Trust marks and frameworks
- Frontiers
  - Interfederation
  - Social2SAML gateways

R&E federations world-wide



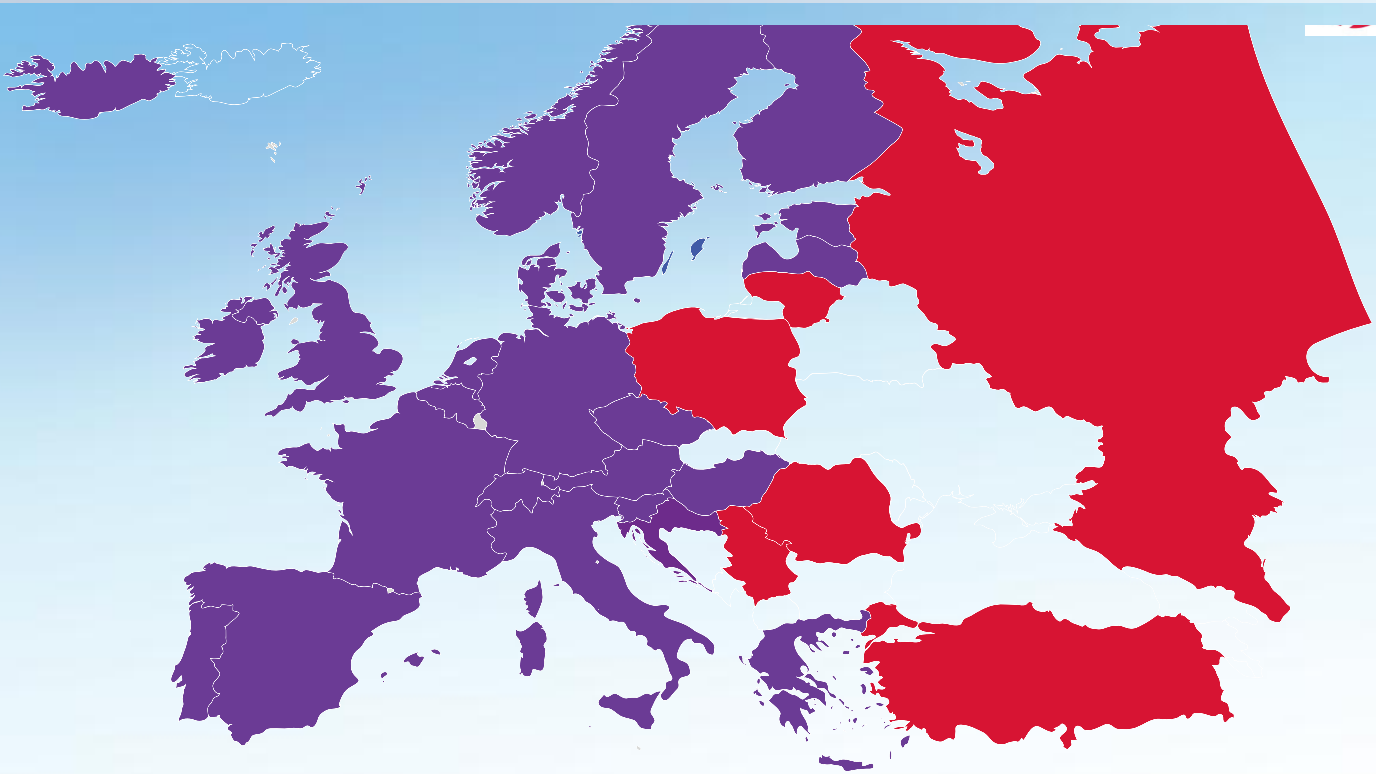
🟪 **Identity Federations in production**

AT	ACOnet Identity Federation	ES	SIR	NL	SURFconext
AU	Australian Access Federation AAF	FI	Haka	NO	FEIDE
BE	Belnet R&E Federation	FR	Fédération Éducation-Recherche	NZ	Tuakiri New Zealand Access Federation
BR	CAFe	GR	GRNET	PT	RCTSaai
CA	Canadian Access Federation CAF	HR	AAI@EduHr	SE	SWAMID
CH	SWITCHaai	HU	eduID.hu	SI	ArnesAAI Slovenska
CL	COFRe	IE	Edugate	UK	UK Access Management Federation for Education and Research
CZ	eduID.cz	IT	IDEM		

🟥 **Identity Federations in pilot**

AR	MATE	PL	PIONIERId
CN	CARSI	RO	RoEduNet Federation
COL	COLFIRE	RS	iAMRES
IN	INFED	RU	ΦEDUrus AAI
LT	LEFT	TR	YETKİM
PE	INCA	ZA	SAIF
MA	eduIDM		
OM	Oman Knowledge ID Federation		

R&E Europe



🟪 **Identity Federations in production**

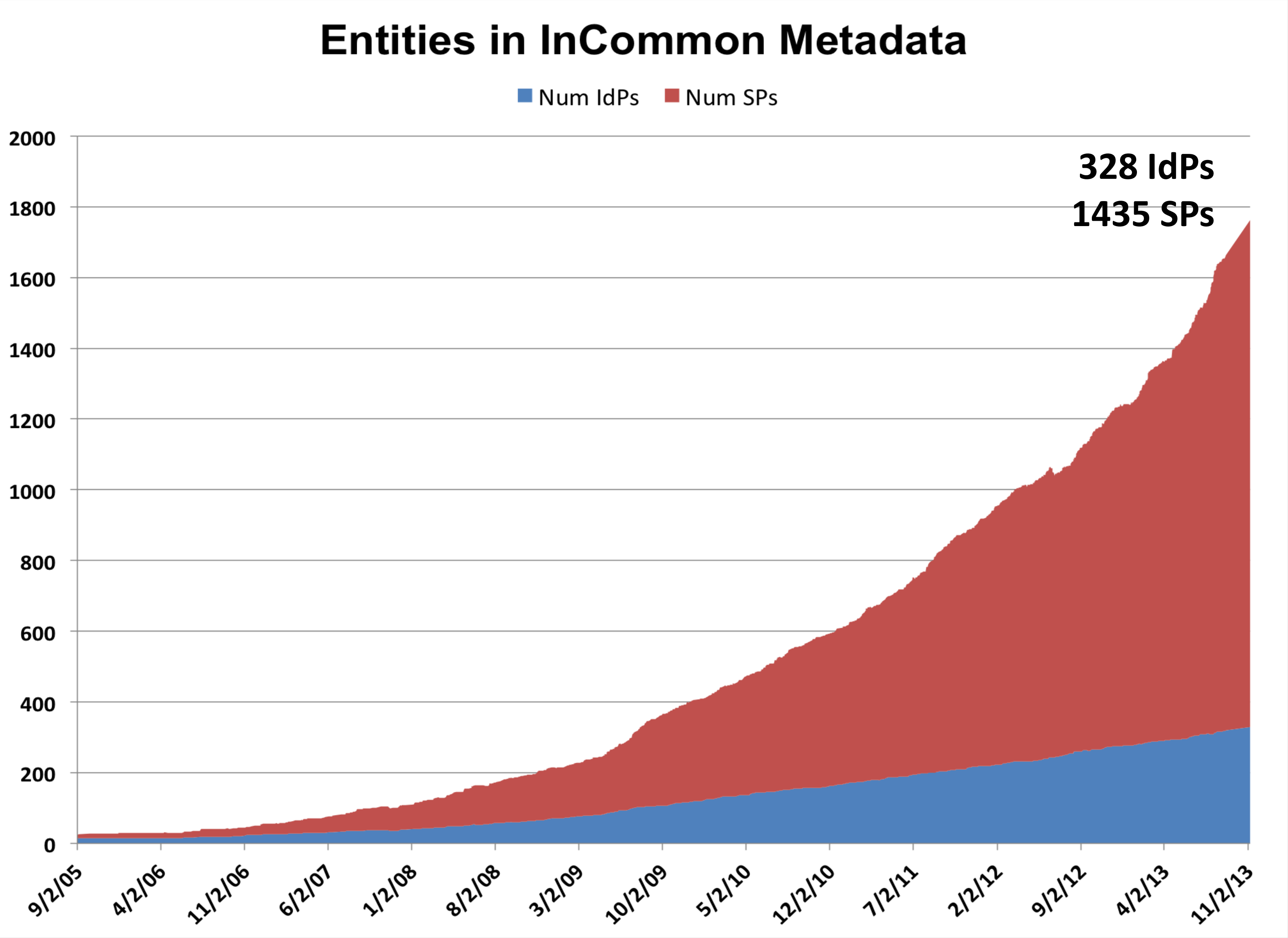
AT	ACOnet Identity Federation	FI	Haka	NL	SURFconext
BE	Belnet R&E Federation	FR	Fédération Éducation-Recherche	NO	FEIDE
CH	SWITCHaai	GR	GRNET	PT	RCTSaai
CZ	eduID.cz	HR	AAI@EduHr	SE	SWAMID

🟥 **Identity Federations in pilot**

CN	CARSI
IN	INFED
LT	LEFT
MA	eduIDM
PL	PIONIERId
RO	RoEduNet Federation

InCommon today

- 400+ universities, 600 + total participants, growth continues strong
  - Many cloud service providers, from Microsoft to Elsevier to NIH and NSF to ***
- > 6-7 M users
- Primary uses:
  - Outsourced services, government applications, access to software, access to licensed content, etc.
  - Access to wikis, shared services, cloud services, calendaring, command line apps, medical, etc.
  - A basic requirement for cloud services
- FICAM certified at LOA 1 and 2 (Bronze and Silver).
- New services
  - Certification marks - R&S (Research and Scholarship)
  - Multi-factor authentication support (devices, software, etc)
  - Certificates – SSL and Personal
  - InCert - open-source client-cert lifecycle management

Entities in InCommon Metadata
Num IdPs
Num SPs
328 IdPs
1435 SPs
2000
1800
1600
1400
1200
1000
800
600
400
200
0
9/2/05
4/2/06
11/2/06
6/2/07
1/2/08
8/2/08
3/2/09
10/2/09
5/2/10
12/2/10
7/2/11
2/2/12
9/2/12
4/2/13
11/2/13

Scalable Privacy

- 2+ year grant to Internet2/InCommon
- Development partners are CMU, Brown, with expertise from Wisconsin, Ohio State and others
- Several focal points
  - Promotion of multi-factor authentication
  - Citizen-centric attributes and schema
  - Development and deployment of privacy managers
  - Introduction of anonymous credentials
- https://spaces.internet2.edu/display/scalepriv

Work described in this presentation is supported by the National Strategy for Trusted Identities in Cyberspace (NSTIC) National Program Office and the National Institute of Standards and Technology (NIST). The views in this presentation do not necessarily reflect the official policies of the NIST or NSTIC, nor does mention by trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Scalable Privacy deliverables

- Promotion of two factor authentication
  - Good privacy begins with good security
- Citizen-centric attribute activities
  - For transactions, for accessibility, for social government
- Trusted metadata approaches
  - About the relying party and the Identity Provider
  - Vetted by the federation and by third-parties
- Next-generation privacy manager
  - Leveraging prior work, trusted metadata, usability-built-in
- Anonymous credentials
  - Evaluate issues in integrated deployments at scale
  - Integration in software, use of metadata, and user experience

Promotion of multi-factor authentication (MFA)

- Good privacy begins with good security
- MFA addresses a significant number of security threats
- A variety of second factor alternatives are now viable – USB devices, NFC devices, cell phones, certificates, etc., and technology can bridge across them
- Advantages of MFA and Federated identity
  - Combining MFA with WebSSO and federated identity allows MFA to be leveraged by many services/SPs; "MFA externalities"
  - Potential to help achieve higher levels of assurance
  - If biometric factors are used, "privacy spillage" limited to IdP

MFA: Two major thrusts

- MFA Pilot Institutions: support wide-scale deployments of MFA technologies at three institutions:
  - Massachusetts Institute of Technology (MIT)
  - University of Texas System
  - University of Utah
- MFA Cohortium: Create and facilitate a cohort of additional institutions, establishing a collaborative environment for sharing questions, requirements, planning, expertise, experience, artifacts, etc. related to deploying and supporting MFA, leveraging the pilot institution activities.
  - Now ~ 40 institutions, > 1M potential users
  - Creating a next generation of MFA aware users
  - Technology agnostic, lifecycle oriented
  - https://spaces.internet2.edu/display/mfacohortium

Early interesting issues in MFA at scale

- Accessibility support
  - From device issues to accessing preferences during MFA processes
- FERPA issues in the release of PII (e.g. cell phone number) to third party authenticator
  - More generally the legal relationship between enterprise and third party authenticators
- Cloud authenticators and DDOS attacks
  - Should enterprise authn fail under external DDOS?
  - Generally, identify key barriers to outsourcing components of authn
- Alternative strategies when multifactor tokens aren’t available
  - MFA fails more frequently, if only for environmental issues
  - “Fallback” approaches for opt-in deployment models?
- ROI of federated MFA
  - The leverage of federation and MFA is enormous, but how to capture it?

Three important software deliverables

- Shibboleth-based integrated, universal MFA handler
  - Shib is the most widely used open source federating software platform in the world
  - Multilateral Shib-based federations exist in over 40 countries, in real estate, in government, in law enforcement, in securities and banking, etc
  - A universal well-integrated MFA handler instantly opens MFA externalities
- CAS integrated, universal MFA handler
  - CAS is a very widely used open source SSO
- InCert
  - Open source client certificate lifecycle management system
  - Also provides device boarding and device security
  - Client certs are invaluable for many ecosystem capabilities beyond authentication and anti-phishing
  - http://www.internet2.edu/incert/
  - https://spaces.internet2.edu/x/vAhOAg

Citizen-centric attribute deliverables

- Schema Catalog and Attribute Registry
  https://spaces.internet2.edu/x/dgROAg
  http://macedir.org/ontologies/attribute/2012-11-10/attributeOntologyDoc/
- Attribute-annotated Use Cases
- Cookbook “To Serve Citizens” ☺
- Global Public Inclusive Infrastructure (GPII) Proof of concept, using User-Managed Access (UMA)
- Bindings and refactoring
- Engagement with the privacy manager

GPII Proof of Concept

- The purpose of the Global Public Inclusive Infrastructure (GPII) is to ensure that everyone who faces accessibility barriers due to ***disability***, ***literacy***, ***digital literacy,*** or ***aging***, regardless of ***economic resources***, can access and use the Internet and all its information, communities, and services for education, employment, daily living, civic participation, health, and safety
- Automatic personalization of user interfaces and user context adaptation based on user preferences, across platforms
- Schema standard is AccessForAll (ISO/IEC JTC1 24751)
- http://gpii.net
- Pilot applications, proofs of concept beginning with
  - User preferences stored and accessed securely in an online repository
  - Those preferences drive presentation features that provide accessibility accommodations when user visits online resources
  - All leveraging UMA profiles of Oauth 2.0 aligned with emerging GPII security and privacy architectures

What we hope to learn in the next year

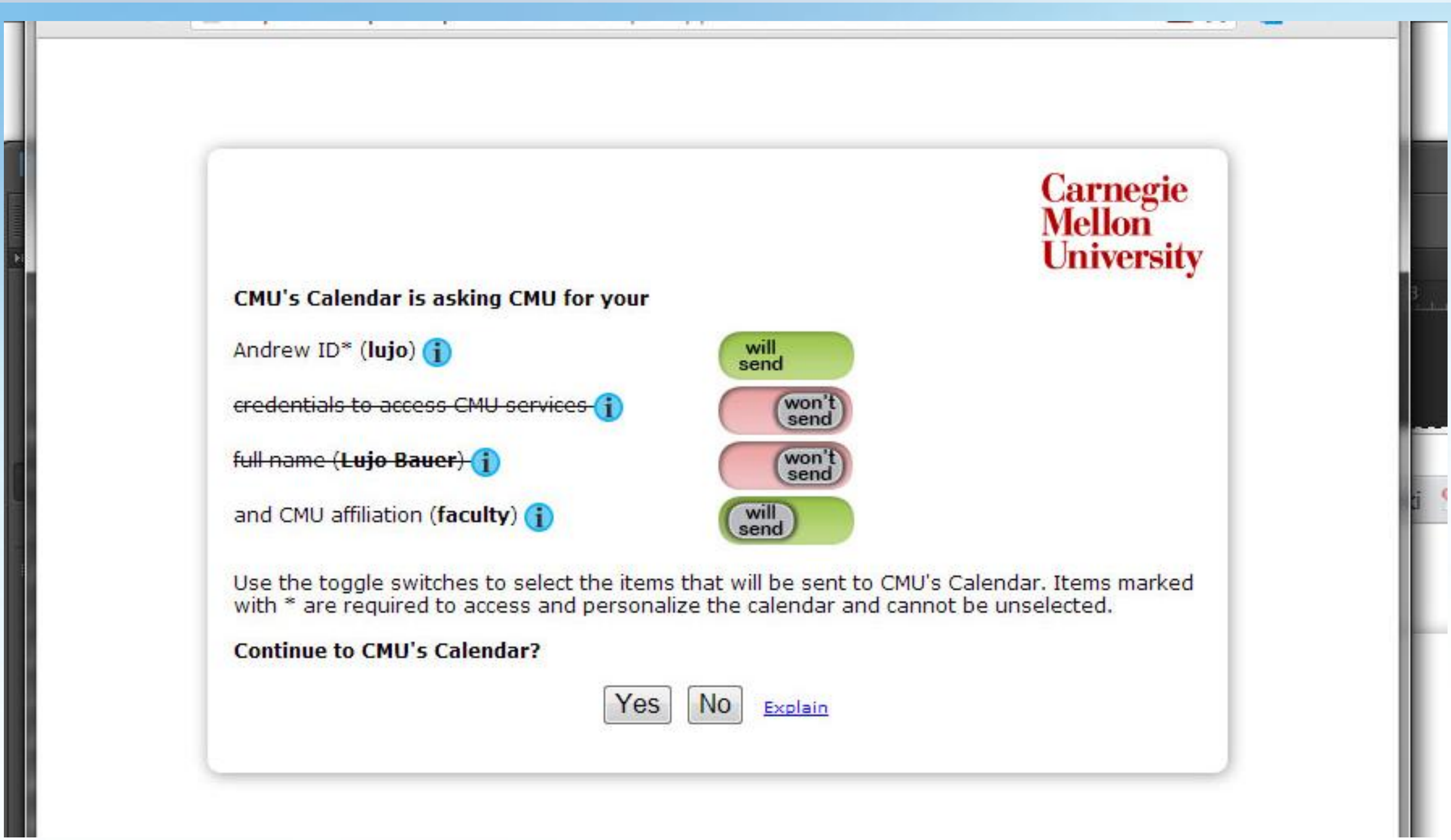
- Annotate additional use cases
- Foster some convergence discussions
- Develop key data-driven issues:
  - In R&E, IdP’s are normalized (syntax and semantics) on key attributes but differ among themselves in privacy policies and what we release to others; in the social space, IdP’s are wildly divergent on attributes but generally promiscuous in which attributes are released.
  - Is there a hierarchical “sweet spot” where users can actively manage privacy with almost no impedance?
  - Internationalization issues, from policy to the Spanish surname topic
- Foster active research on usability within the academic community
- The relationship of citizen-centric attributes to provisioning data

Privacy managers (Carnegie-Mellon University)

- Consoles to help users manage the release of attributes
- Can leverage trust, informed consent, default settings and preferences, etc.
- Must be carefully engineered
  - Across the variety of contexts
  - Across a variety of credential types
  - In ways that are user-effective
- Similar, less leveraged approaches are successfully deployed in a few settings, demonstrating that users can and will manage privacy.
- Research shows that over 90% of social network users do not know what attributes are being released or how to change it

Key design considerations

- Usability
- CMU Tech Report, Warning Design Guidelines, Bauer et al
- Informed and * consent
- GPII
- Technology agnostic – SAML, anon creds, OpenId, etc., though plumbed to Shib to start
- Awareness of out-of-band considerations
- “Nudging” applied to privacy
- Minimal disclosure for constrained purpose
- First alpha due this month



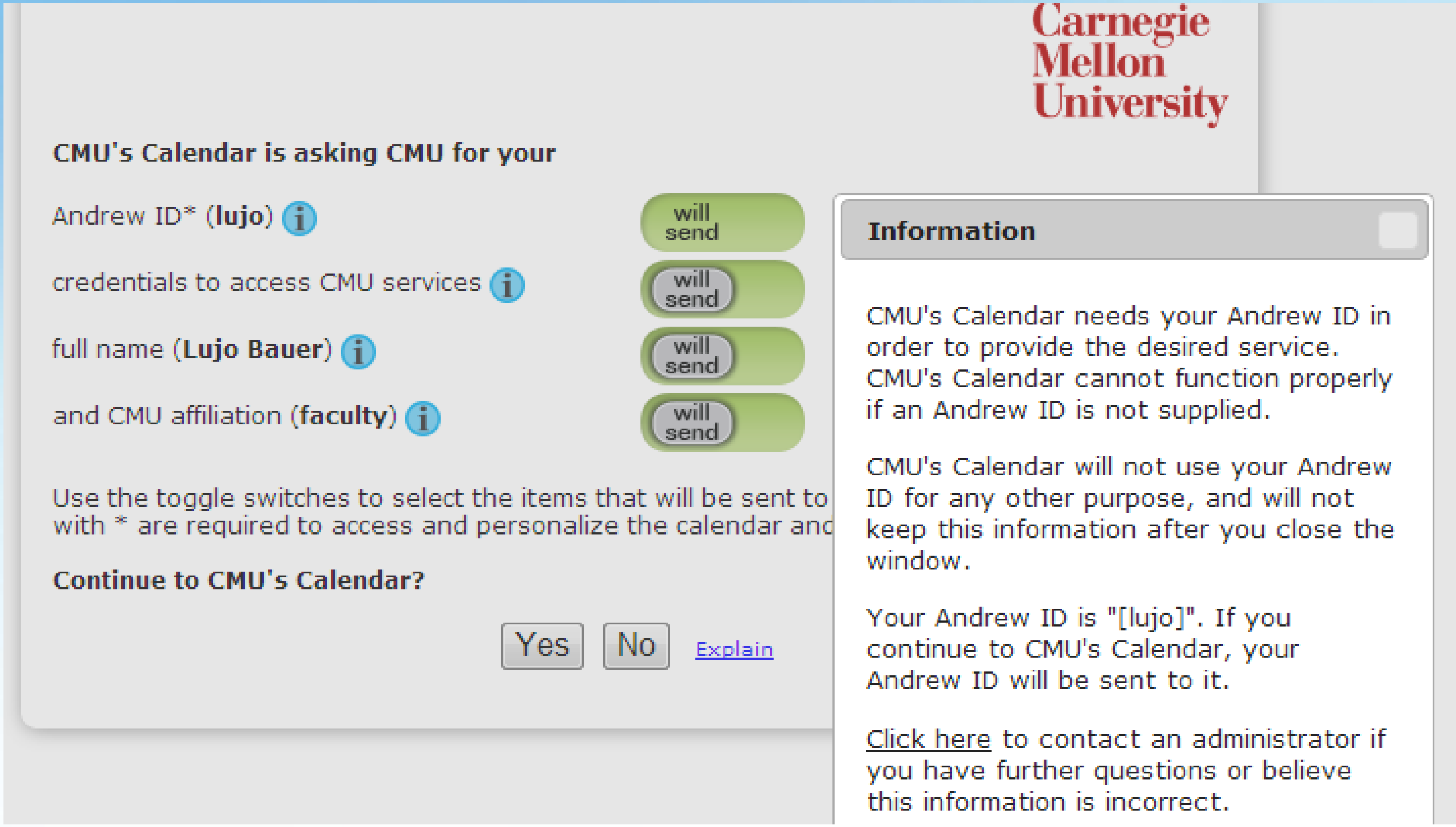
Carnegie Mellon University

CMU's Calendar is asking CMU for your

Andrew ID* (**lujo**) ⓘ	will send
~~credentials to access CMU services~~ ⓘ	won't send
~~full name (**Lujo Bauer**)~~ ⓘ	won't send
and CMU affiliation (**faculty**) ⓘ	will send

Use the toggle switches to select the items that will be sent to CMU's Calendar. Items marked with * are required to access and personalize the calendar and cannot be unselected.

Continue to CMU's Calendar?



Carnegie Mellon University

CMU's Calendar is asking CMU for your

Andrew ID* (**lujo**)

credentials to access CMU services

full name (**Lujo Bauer**)

and CMU affiliation (**faculty**)

Use the toggle switches to select the items that will be sent to with * are required to access and personalize the calendar and

Continue to CMU's Calendar?

Information

CMU's Calendar needs your Andrew ID in order to provide the desired service. CMU's Calendar cannot function properly if an Andrew ID is not supplied.

CMU's Calendar will not use your Andrew ID for any other purpose, and will not keep this information after you close the window.

Your Andrew ID is "[lujo]". If you continue to CMU's Calendar, your Andrew ID will be sent to it.

Click here to contact an administrator if you have further questions or believe this information is incorrect.

Metadata and trust implications

- At scale, there needs to be ways to establish and convey trusted information about applications and services to users
  - Implies "vetting" or auditing processes for services
  - Implies metadata that can convey this information in real time to users
  - Implies trust in the metadata
- Dynamic metadata services
  - Work is already underway on this in other places
- Federation operations need to evolve
- Auditing applications
  - For "privacy-preserving" approaches (minimal attribute requests, informed consent, proper handling and disposal, etc.), for COPPA compliance, for …
  - Prototype approaches are successful; market needs to grow

Anonymity, unlinkability, and unobservability

- *Anonymity* assures that public data cannot be related to the owner.
- *Unlinkability* assures that two or more related events in an information processing system cannot be related to each other.
  - *Untraceability* assures that two or more events at autonomous systems by the same user cannot be correlated
- *Unobservability* assures that an observer is unable to identify or infer the identities of the parties involved in a transaction.

Anonymous Credentials

- Special credentials issued by attribute authorities
- Allows for minimum disclosure of attributes of bearer
  - Over legal age; graduate of university in year X; resident; first-responder certifications; access to age-restricted services; etc
- Can develop trusted responses to access policy by processing previously obtained credentials
  - Eg. Age > 21 developed from birthdate
  - Can use multiple credentials as input when responding
  - Responses optionally contain original attribute values
- Built on several similar technologies, including ABC4Trust (funded by the EU) and uProve (open licensed from MS)
- Tamper-proof
- Unobservable
- Long-time cool technology in search of use cases and modern enhancements (mobility, informed consent, etc.)
- Several pilots looking at integrating them in various ways
- Our work is being led by Brown University

Deployment Models

- Classic ABC4Trust, Idemix, etc.
  - Credentials held in a cert store on the user's desktop or smart card
  - RPs accessed via Web Browser
  - Processing done in User's desktop by previously downloaded plugins
- Enterprise-based
  - Credentials held in enterprise directory
  - Processing still done in desktop
  - Addresses mobility
  - May serve important enterprise needs
- Cloud-based
  - Processing and storage moved to the cloud
  - Addresses mobility issues, new devices
- Card based
  - Some way cool smartcard based Dutch work
  - http://www.irmacard.org

What we’ve learned about anon creds

- Badly misnamed technology
  - Can provide identity info, with user consent
  - Provides for minimal disclosure of attributes
  - Lots of alt approaches that use similar phrases such as zero-knowledge, anonymous credentials, double blind gateways, etc.
- The open source is not ready for prime time; the proprietary implementations have lots of issues
- Adding modern features such as mobility and * consent affects trust issues and are poorly addressed
- Deployment model influences trust model
- Still appear to be the best answer for *unobservability*
- Abc4Trust has Inspector mechanism, under user control, allowing for “opening” a policy response

Of trust frameworks, marks and elements

- Trust frameworks and trust marks are ambiguous and misconstrued terms.
- What we have some understanding of is many of the trust elements that can be used, in concert, to build frameworks and marks.
- The elements fit well into a periodic table showing the issues (e.g. legal, privacy, operational) that they address
- There are new elements still be discovered, and the organization of the table is malleable
  - E.g. Hub and spoke versus multi-lateral federations

Aspects of the Periodic Table

- Most current version of the periodic table is athttps://spaces.internet2.edu/display/scalepriv/
- Rows represent scale, from the relatively few federated operators at the top to the thousands of organizations and millions of users at the bottom
- Colors represents business functional areas, including technical, operational, policy, legal, etc.
- Clusters of elements represent related sets of issues, such as the technical requirements needed to trust attribute authorities within a federation

Interfederation

- The steady state of federated identity is “interfederated identity”
- Interfederation across countries in the same vertical.
- Interfederation between sectors (R&E and K-12; R&E and healthcare; R&E and government).
- Key technology change is the move from static metadata bundles (ala /etc/hosts) to dynamic metadata (ala DNS)
  - Standards and code are now moving forward
  - Exchange points are being shaped
- Key policy issues are in the periodic table –
  - E.g. Europe is advancing adjudication in the identity provider country; every SP in the US could be challenged.
  - Privacy issues are particularly hard

Social2SAML

- Social2SAML gateways
  - Converts social identities (e.g. Google, Yahoo, MSN, Facebook) into SAML assertions
- Exposes many issues with social identity that require careful thought.
  - Conversion of identifier types
    - Implications of persistency, etc
  - What's in a name
  - Promiscuous attribute release
  - LOA mapping
- Very handy for extended populations

Takeaways

- Moving the needle on MFA
  - A number of important, solvable issues are emerging
- Attributes are the key and its already a mess
- Researching what it takes to put the “informed” into consent, and trying to build it
- Anonymous credentials are still immature, and still the only answer to unobservability
- New businesses, such as application auditing, are needed
- The real steady state future is “interfederated identity” but getting there is getting harder